CLAIMS

What is claimed is:

1. A method of providing secure communication between a remote system and a remotely accessed system, comprising:

calculating at the remote system a first hash of an operation using a hash algorithm;

encrypting at the remote system the first hash to form a signed hash;

receiving at the remotely accessed system the signed hash from the remote system;

storing at the remotely accessed system a reference hash in a section of non-volatile memory before receiving the signed hash;

validating at the remotely accessed system the signed hash using the reference hash; and

executing at the remotely accessed system the operation associated with the signed hash if the signed hash is validated.

2. The method, as set forth in claim 1, comprising responding to the remote system based on the validation of the signed hash.

3. The method, as set forth in claim 2, wherein responding to the remote system comprises generating a completion message if the signed hash is validated.

4. The method, as set forth in claim 2, wherein responding to the remote system comprises generating an error message if the signed hash is not validated.

5. The method, as set forth in claim 1, wherein the operation comprises a command.

6. The method, as set forth in claim 1, wherein the operation comprises identification information.

7. The method, as set forth in claim 1, wherein validating comprises accessing a database to access the reference hash.

8. The method, as set forth in claim 1, wherein validating comprises parsing a packet to access the signed hash.

9. A method of providing secure communication between systems, comprising:

delivering identification information to a remotely accessed system from a remote system;

creating a nonce at the remotely accessed system;

delivering the nonce to the remote system;

calculating at the remote system a first hash of an operation using a hash algorithm;

encrypting at the remote system the first hash along with the nonce to form a signed hash;

receiving at the remotely accessed system the signed hash from the remote system;

storing at the remotely accessed system a reference hash in a section of non-volatile memory before receiving the signed hash;

validating at the remotely accessed system by comparing the signed hash to the reference hash; and

executing at the remotely accessed system the operation associated with the signed hash if the signed hash is validated.

10. The method, as set forth in claim 9, wherein encrypting comprises signing at the remote system the first hash to form the signed hash.

11. The method, as set forth in claim 9, comprising parsing at the remotely accessed system a packet for the first signed hash.

12. The method, as set forth in claim 9, comprising responding to the remote system based on the validation of the signed hash.

13. The method, as set forth in claim 9, wherein generating the nonce at the remotely accessed system comprises storing the identification information at the remotely accessed system and validating comprises verifying the identification information to determine if a packet is valid.

14. The method, as set forth in claim 9, wherein validating comprises accessing a database for the reference hash, wherein the reference hash comprises a second hash along with the nonce.

15. The method, as set forth in claim 9, wherein validating comprises accessing a database for the reference hash, and combining the reference hash with the nonce to validate the operation from the remote system.

16. The method, as set forth in claim 9, wherein validating comprises verifying the identification information.

17. The method, as set forth in claim 9, wherein generating the nonce at the remotely accessed system comprises storing the nonce at the remotely accessed system and validating comprises verifying the nonce in a packet.

18. A system comprising:

a first computer system, the first computer system comprising a first program for hashing information;

a request being generated from information received by the first computer system and hashed by the first program;

a network connected to the first computer system and adapted to receive the request;

a second computer system connected to the network and adapted to receive the request from the first computer system, wherein the second computer system comprises:

a processor;

a first section memory operatively coupled to the processor, the first section memory storing a file that is a hash; and

a second section of memory being configured to store a validation program initiated by the processor, the validation program having a validation routine configured to validate the file stored in the first section of memory against the received request; wherein if the received request is valid, the second computer system may execute a command that corresponds to the file.

19. The system, as set forth in claim 18, wherein the information comprises a command.

20. The system, as set forth in claim 19, wherein the information comprises a nonce.

21. The system, as set forth in claim 18, wherein the first computer system comprises a second program for digitally signing information.

22. The system, as set forth in claim 21, wherein the validation program compares the hash stored in the first section of memory against signed information in the received request.

23. The system, as set forth in claim 22, wherein the signed information comprises a signed command and signed argument.